International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET22966

A Modern mechanism for Generating 3DES Algorithm Keys Based on Rubik's Cube

Saadi Mohammed Saadi
Ministry of Education, Bagdad-Iraq

Article Info
Volume 9, Issue 6
Page Number : 180-188

Publication Issue :
November-December-2022

Article History
Accepted : 07 Nov 2022
Published: 20 Nov 2022

ABSTRACT

Encryption makes a message incomprehensible to the reader and difficult for unauthorized individuals to access. One of the most serious issues we face is the key, which plays a crucial role in secure communication and is critical to the encryption process. To enhance the level of security, the key of any algorithm must be vital, and the secret key used must be a copy of it at both the sending and receiving ends. This type of encryption is known as symmetric encryption and must be secure. In this paper, the key of one of the symmetric encryption techniques, the 3DES Algorithm, will be reconfigured to make the algorithm more secure, faster, and more robust. The results obtained from this paper also have good resistance against brute force attacks, which makes the system more efficient by applying the improved algorithm where the message is encrypted and decrypted faster, making the attacker difficult to hack the encrypted message. The proposed method has been programmed in VisualBaic.Net 2015.

Keywords: Triple DES, Cryptography, Rubik's Cube, Decryption, and Encryption.

I. INTRODUCTION

Improved technology in the field of the internet triggers the occurrence of problems, especially in the area of Internet security. Since Internet media users are relatively high, Internet crimes may occur in sending data through internet media. Among these are file modifications or the theft of essential data transmitted over the internet [1]. By using security services like confidentiality, authentication, data integrity, and non-repudiation, encryption is necessary to ensure a secure exchange of data. The term "data confidentiality" refers to the practice of preventing unauthorized parties from accessing sensitive data. Cryptographic methods have traditionally included several mathematical and logical elements [2], [3], [4]. The challenges imposed by cryptanalysts who are constantly attempting to break any encryption system make it difficult to develop a completely secure encryption algorithm. To satisfy the high-security requirements and safeguard cryptographic components from cryptanalysis, choosing the right cryptographic algorithm is essential. [5]. In this context, a key schedule algorithm produces secret keys and is crucial for creating encryption schemes. To develop a robust and substantial key generation process that makes it more difficult for a cryptanalyst to obtain the secret key and to thwart the related key attack, numerous different kinds of studies have been conducted [6]. Figure 1 illustrates how to send an encrypted message by having the sender encrypt the secret key before sending it to the recipient, who will then use the private key to decrypt the message. Data privacy and data integrity are among the security objectives that are provided through encryption, among others. Since encryption offers tremendous security advantages, it is frequently used nowadays [7].

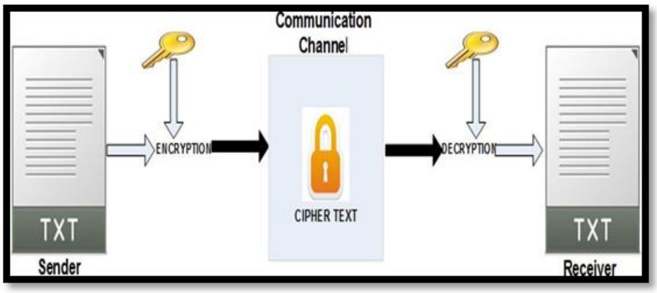


Figure 1 : Encryption and decryption work [7].

II. CLASSIFICATION OF CRYPTOGRAPHY

The two fundamental processes in cryptography are encryption and decryption. When a message is encrypted, it transforms from plain text into cipher text, which is unintelligible. Messages are protected using these two features from viewers who are not authorized to view their content [7].

Asymmetric cryptography and symmetric key cryptography are two major categories into which the encryption algorithms are divided [7].

A. Symmetric key cryptography

The simple operation of the encryption and decryption mechanisms is shown in Figure.1. Public key cryptography, also known as asymmetric cryptography, secures communication by using both public and private keys. Secure communication between sender and recipient using the same secret key is the aim of symmetric cryptography, also known as symmetric key cryptography[8]. All users have access to the public key because it is open, but the private key is kept private. Blowfish, Triple Data Encryption Standard, Advanced Encryption Standard (AES), and Data Encryption Standard (DES) are just a few of the numerous unique proprietary algorithms (3DES) [9].

B. Asymmetric cryptography

To secure the connection, this type of encryption, also referred to as public key encryption, encrypts data using one key (the "public key") and decrypts it using a different key (the "private key") There are numerous variants of generic algorithms, in addition to the generic algorithm, the Rivest Shamir Adleman (RSA) algorithm, ECC, and the Digital Signature Algorithm (DSA) [10]. Figures 2 and 3 illustrate symmetric and asymmetric cryptography, respectively.

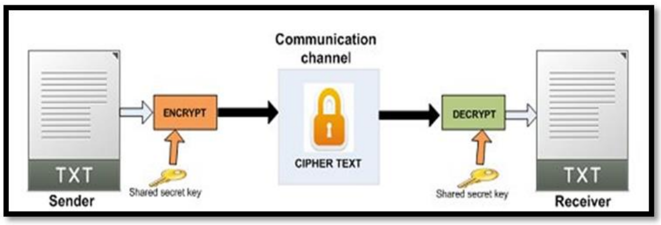


Figure 2. Symmetric encryption [7].

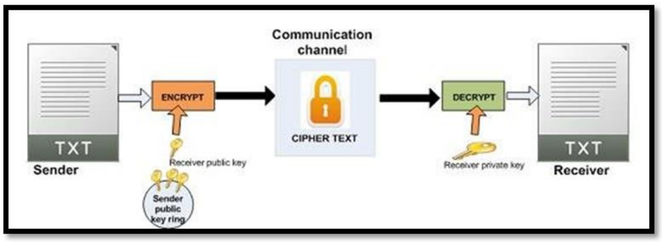


Figure.3. Asymmetric encryption[7].

III. Overview of cryptographic algorithms:

The algorithms 3DES and Rubik's Cube Algorithm, which will be covered in this part, were employed in this study.

A. 3DES (Triple Data Encryption Standard Algorithm).

A cipher block type is used in the symmetric cryptography technique 3DES. A symmetric encryption scheme employs a single key that can be used for both encryption and decryption. Additionally, a cipher block is a form of asymmetric encryption that has a fixed or fixed bit size; for DES, this size is 64 bits [11]. To increase DES security, the Double DES algorithm was developed into 3DES. The ordinary DES cipher is used three times in the Triple DES algorithm. It is given a 168-bit secret key divided into three keys of (56) bits each key length

- In the first stage, the encryption is with the initial secret key
- In the second stage, the decryption is based on the k2 secret.
- In the third stage the encryption is based on the k3 secret.

Encryption: C = E3 (D2 (E1 (m))), Decryption: m = D1 (E2 (D3 (C)).

The decryption allows the second step of encryption to be compatible with the versions Previously with the widely used DES algorithm. In some cases, k1 and k2, or k2 and k3, are the same.

(D1 (E1 (m)) = E3, C = E3 (m) (D3 (E1 (m)) = E1 where C = (m) Using a unique 112-bit key, The 3DES cipher is an option. In this case, the two secret keys (k 1 and k3 are the same. The encryption will be as follows

C = E1 (D2 (E1 (m))). Triple DES is advantageous due to its large key length, which is longer than the majority of key lengths associated with ciphers. 3DES encryption with two or three distinct keys is still considered reliable for use today [12]. The block diagram for 3DES is shown in Figure 4 below.

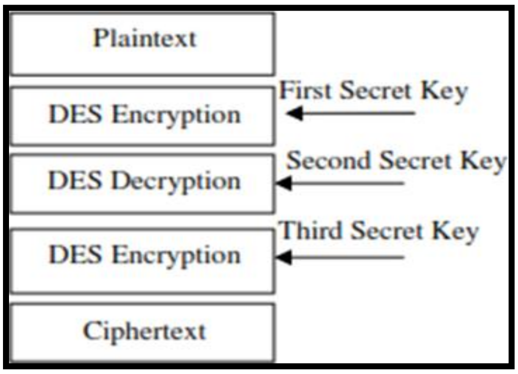


Figure 4 : Block diagrams for 3DES encryption [12]

B. Algorithm for the Rubik's Cube:

It is a three-dimensional structure toy that assesses a person's knowledge and skills. Erno Rubik created it in 1975[13]. It was one of the best-selling video games as of 2009, with more than 350 million units distributed globally. Numerous Rubik's Cube-based techniques for encoding text or images have been developed because of the striking similarity between the permutation of the Rubik's Cube and cipher [14, 15, 16, 17].

As shown in Figure 5, it is possible to design or alter the Cube so that it does not obstruct the body's rotation. By the end of 2013, the Chinese company Sheng Shou was manufacturing cubes in all sizes, from 2 x 2 x 2 to 10 x 10 x 10 [18,19]. There are six examples of the particularly shaped Cube in Figure 6. They come in various structural configurations, such as the multi-faceted Cube, the spherical Cube, the tetrahedral Cube, the mirror Cube, the gear Cube, etc.

Figure 5 : The most recent Rubik's Cube [19].

The Rubik's Cube was constructed based on how many times each face could wrap around its center, as shown in Figure 6.

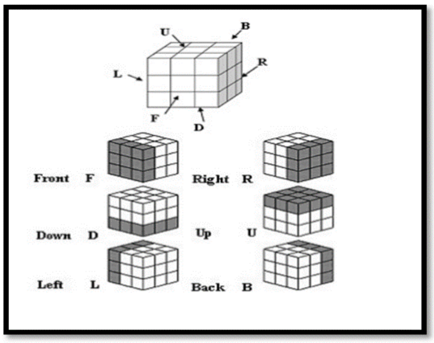


Figure 6 : Rubik's Cube [19].

IV. Framework for the proposed method:

In this section, we'll cover the process for creating keys for the 3DES Algorithm, which creates an array called a Rubik's Cube made up of 16 letters or digits. The improved 3DES algorithm is used to encrypt the message before being decoded to reveal the original text, as shown in the framework for the proposed method in Figure 7. Simply pressing on it generates a key from which we derive the three keys of this algorithm, where every throw, a new number is generated that is explained.

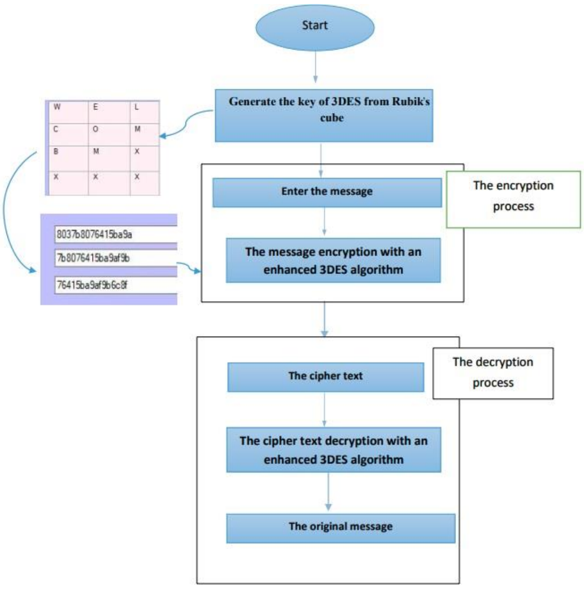


Figure 7. Framework for the proposed method

V. Methodology The proposed method and its implementation

The key generation stage, the encryption process stage, and the decryption process stage are all included in the three steps of the proposed system. The three stages, corresponding to the key generation stage, the encryption stage, and the decryption stage, respectively, according to the framework shown in the previous figure, will be described by the method proposed in the paper as in Figures 10, 11, and 12, and The suggested method is illustrated in Figure 8.

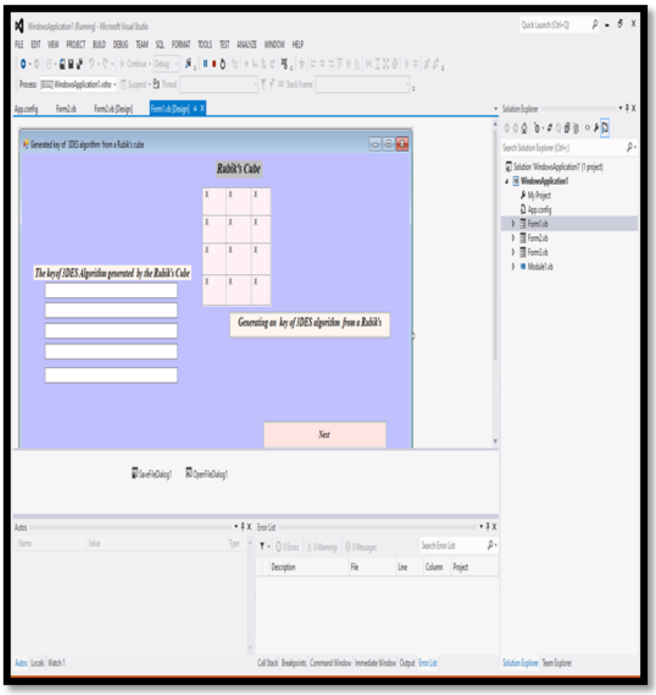
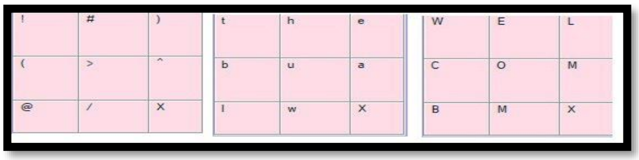

WindowsApplication1 (Running) - Microsoft Visual Studio
FILE EDIT VIEW PROJECT BUILD DEBUG TEAM SQL FORMAT TOOLS TEST ANALYZE WINDOW HELP
App.config
Form2.vb
Form2.vb [Design]
Form1.vb [Design]
Generated key of 3DES algorithm from a Rubik's cube
Rubik's Cube
X X X
X X X
X X X
X X X
The key of 3DES Algorithm generated by the Rubik's Cube
Generating an key of 3DES algorithm from a Rubik's
Next
SaveFileDialog1
OpenFileDialog1
Solution Explorer
WindowsApplication1
Autos
Error List

Figure 8. The window of the suggested method Main.

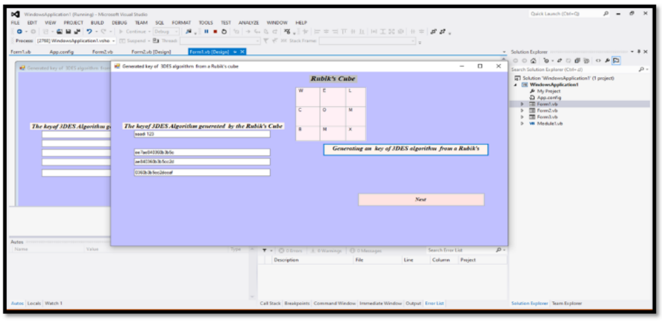
A. The key generation phase:

The method presented here typically describes a 3D matrix's cubic structure. In this paper, we depict the six sides of the Rubik's cube base as well as its six faces, with (U) standing for the top, (D) for the bottom, (L) for the left, and (R) for the right, as well as forward (F) and back (B). In this study, faces were counted, which is a matrix of (33), the number of faces in the cube is (6), the number of cells formed in one face (54), and the length of each key (56). It was calculated to add up to three keys, or 162, but in practice, the key size is 168 to accommodate three keys and their full length. It is difficult to guess these keys using brute force attacks because it is difficult to organize the cube, which is impossible for an attacker to predict the key and know or derive the key from. To achieve a key size of up to 168, the dice are rolled four times with the fourth roll being six bytes short. It will also be difficult to predict the fourth roll from which it will be derived. As shown in Figure 10, the interface that participated in the proposed configuration included the completion of the length of the remaining keys. The key generation method as a model of the proposed work represents the method of generating the key from a Rubik's Cube. Figure 9 illustrates the key generation method.



!	#	)	t	h	e	W	E	L
(	>	^	b	u	a	C	O	M
@	/	X	l	w	X	B	M	X

Figure 9. Face a Rubik's Cube to generate keys.



WindowsApplication1 (Running) - Microsoft Visual Studio
FILE EDIT VIEW PROJECT BUILD DEBUG TEAM SQL FORMAT TOOLS TEST ANALYZE WINDOW HELP
Form1.vb App.config Form2.vb Form2.vb [Design] Form1.vb [Design]
Generated key of 3DES algorithm from a Rubik's cube
Rubik's Cube
W E L
C O M
B M X
Generating an key of 3DES algorithm from a Rubik's
Next

The keyof 3DES Algorithm generated by the Rubik's Cube

saadi 123

ee7ae840360b3b5c

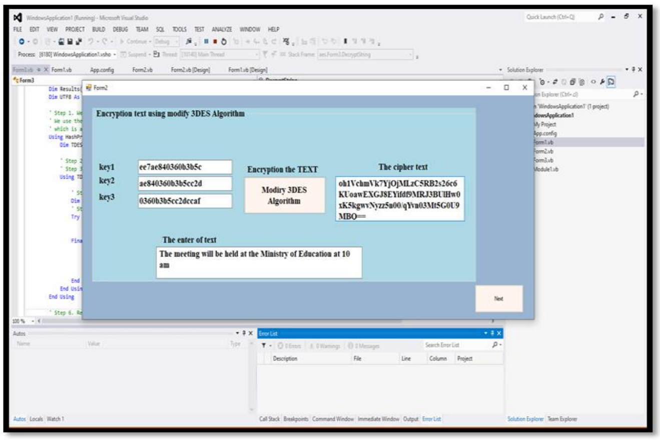
ae840360b3b5cc2d

0360b3b5cc2dccaf

Figure 10. Generate 3DES algorithm keys from Rubik's Cube.

B. Stage of Encryption:

The Rubik's Cube keys encrypt the clear text containing the following message. "The meeting will be held at the Ministry of Education at 10 a.m." its cipher text is " oh1VchmVk7YjOjMLzC5RB2s26c6KUoawEXGJ8EYifdf9MRJ3BUlHw0xK5kgwvNyzz5n00/qYvn03Mt5G0U9MBQ== " The message output is encoded using the enhanced 3DES algorithm built on the Rubik's cube. as shown in Figure 11.



WindowsApplication1 (Running) - Microsoft Visual Studio
FILE EDIT VIEW PROJECT BUILD DEBUG TEAM SQL TOOLS TEST ANALYZE WINDOW HELP
Form2
Encryption the TEXT
Modiry 3DES Algorithm
Next
Error List
Description File Line Column Project

Encryption text using modify 3DES Algorithm

key1 ee7ae840360b3b5c

key2 ae840360b3b5cc2d

key3 0360b3b5cc2dccaf

The cipher text

oh1VchmVk7YjOjMLzC5RB2s26c6KUoawEXGJ8EYifdf9MRJ3BUlHw0xK5kgwvNyzz5n00/qYvn03Mt5G0U9MBO==

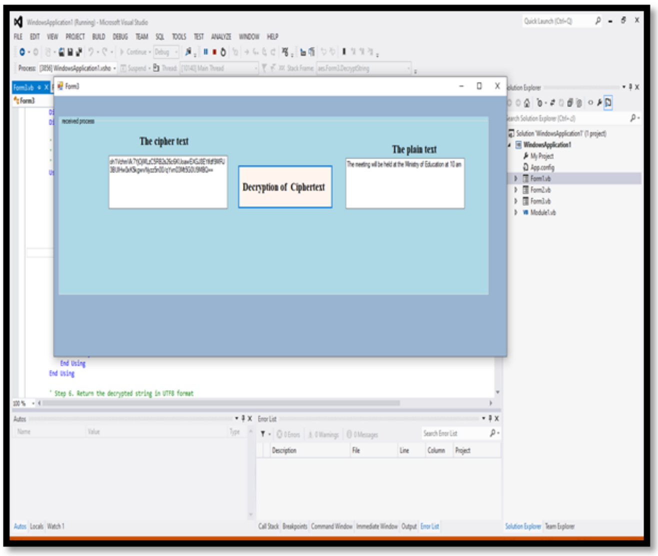
The enter of text

The meeting will be held at the Ministry of Education at 10 am

Figure 11. The encryption stage employs Improved 3DES Algorithm.

C. Decryption Stage:

Finally, the original text is retrieved using the improved 3DES algorithm as shown in Figure 12.



WindowsApplication1 (Running) - Microsoft Visual Studio
FILE EDIT VIEW PROJECT BUILD DEBUG TEAM SQL TOOLS TEST ANALYZE WINDOW HELP
Form3
received process
Decryption of Ciphertext
Error List
Description File Line Column Project

The cipher text

oh1VchmVk7YjOjMLzC5RB2s26c6KUoawEXGJ8EYifdf9MRJ3BUlHw0xK5kgwvNyzz5n00/qYvn03Mt5G0U9MBQ==

The plain text

The meeting will be held at the Ministry of Education at 10 am

' Step 6. Return the decrypted string in UTF8 format

Figure 12. The improved 3DES algorithm is used in the decryption phase.

VI. Results and Discussion:

Because changes in speed and security occur when any process or line of the algorithm code is modified, optimizing the performance of the cipher algorithm necessitates numerous tests on the speed of encryption and decoding, as well as extensive analysis of the level of security. The algorithm must also be tested with various file sizes and types (for example, text and images) to ensure comprehensiveness. It can encrypt any size and most types of files and compare the improved algorithm method with the traditional way with file types, with the enhanced process showing the best results in terms of encryption and decryption time. Increase productivity while also increasing safety.

A. Speed and performance metrics

In this part, we will explain the most important measure of the speed and performance of the algorithm, which are:

1. Encryption time, which is one of the performance metrics, is the length of time needed by the encryption algorithm to transform readable plaintext into unintelligible cipher text.

2. Decryption Time: It is the inverse measurement of cipher time, the time it takes for an encryption algorithm to convert the ciphertext from ciphertext to clear**.**

3. The throughput:

The performance of the algorithm improves and becomes more efficient as the throughput value increases.

Throughput = exact text size in bytes / encoding time in seconds.

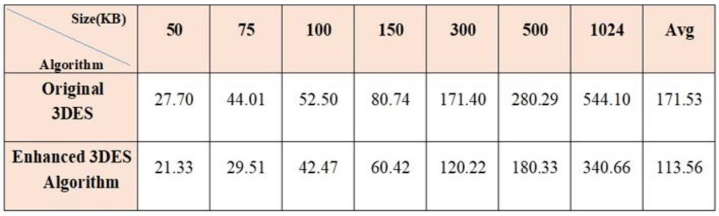
4. Security Level:

It is a set of tests conducted on the encryption algorithm and its strength and durability against known attacks. One of the essential elements of the security level scale is the linear correlation coefficient and the rate of the collapse effect, in addition to the length of the key.

B. Text Encryption Tests:

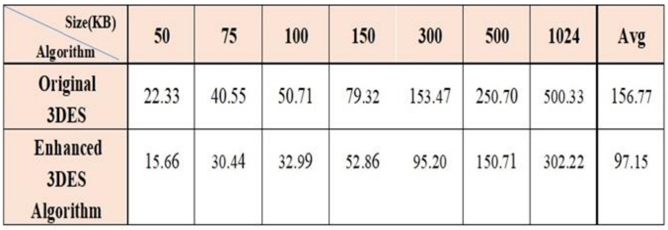
The suggested method tested several text files of different sizes. Tables 1, 2, and 3 show the test results in terms of encoding time, decoding time, and throughput, as well as the difference between the traditional method and the improved 3des algorithm method.

Table 1 - Times for Encryption for Various Text Sizes (milliseconds)



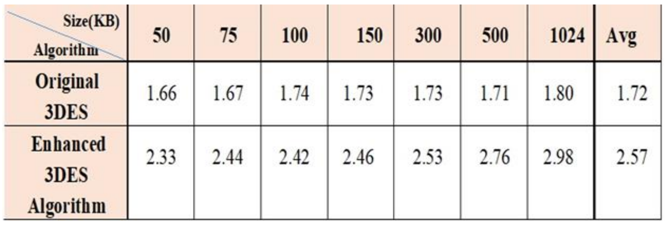
Size(KB) / Algorithm	50	75	100	150	300	500	1024	Avg
Original 3DES	27.70	44.01	52.50	80.74	171.40	280.29	544.10	171.53
Enhanced 3DES Algorithm	21.33	29.51	42.47	60.42	120.22	180.33	340.66	113.56

Table 2- Times for Decryption for Various Text Sizes (milliseconds)



Size(KB) / Algorithm	50	75	100	150	300	500	1024	Avg
Original 3DES	22.33	40.55	50.71	79.32	153.47	250.70	500.33	156.77
Enhanced 3DES Algorithm	15.66	30.44	32.99	52.86	95.20	150.71	302.22	97.15

Table 3 - Throughput for various text sizes (Sec/MB).



Size(KB) / Algorithm	50	75	100	150	300	500	1024	Avg
Original 3DES	1.66	1.67	1.74	1.73	1.73	1.71	1.80	1.72
Enhanced 3DES Algorithm	2.33	2.44	2.42	2.46	2.53	2.76	2.98	2.57

The results above indicate that the suggested method increased throughput while enhancing the performance of the original 3DES algorithm by speeding up encryption and decryption. Before using Rubik's Cube to generate the keys, it was about 53%, 6% less than the proposed new method. However, until security criteria tests are used to determine a fair assessment of the level of security, we cannot be sure that the proposed method is better. Table 4 displays the original algorithm's performance improvement ratios when using the new algorithm after creating the algorithm keys based on the Rubik's cube.

Table 4 The original Algorithm's performance enhancement ratios.

The Method	Increase throughput (MBytes) over 3DES	Speed improvement percentage
Original 3DES	0.62	47.25%
Enhanced 3DES Algorithm	0.75	53.54%

C. Level Security Tests:

The proposed method was tested through a test to measure the level of safety using the correlation coefficient test, as shown in the two test tables **5,6**

Table 5 Distribution of Test Samples among Correlation Domains.

Field / Method	[1.0,0.7]	[0.3,0.7]	[0,0.3]	[-1.0,-0.7]	[-0.7,-0.3]	[-0.3,0]
	Strong relationship	Medium relationship	Weak relationship	Strong relationship	Medium relationship	Weak relationship
Original 3DES	23	210	282	23	170	280
Enhanced 3DES Algorithm	32	170	281	28	200	290

Table 6 Linear correlation coefficient between the original 3DES Algorithm and the improved 3DES Algorithm.

Algorithm	correlation coefficient		
	Strong	Medium	Weak
Original 3DES	5.4%	36.3%	58.3%
Enhanced 3DES Algorithm	6.4%	36.3%	57.3%

Before examining the previous table, we must know that the larger the ratio of the weak linear relationship, the better, and vice versa with the strong linear relationship, the lower the ratio, the better, which makes it difficult for attackers to attack the analysis. From Table 6, I find several results (note that 1% means ten samples, which are:

- The original algorithm gives good results regarding the correlation coefficient, as 58.3% of the samples have a weak relationship. In comparison, samples with a strong relationship do not exceed 5.4% of the total samples.

- Concerning the newly suggested technique, we discover that 1% more strong links exist than with the original algorithm after generating the keys based on Rubik's Cube. In comparison, it falls by 1% in weak ties.

VII.CONCLUSION

The rate increased by 53.54% after using Rubik's Cube to generate keys, demonstrating that the new approach outperforms the old one in terms of productivity, encryption, and decryption speed, resulting in lower battery consumption.Table7 compares the performance improvements in speed and security testing for the correlation coefficient criterion between the original and enhanced 3DES algorithm methods. Figures 13, 14, and 15, respectively, show the time of encryption, decryption, and throughput in milliseconds.

Table 7 : Comparison of the original and improved 3DES algorithms in terms of speed performance and security level

Algorithm	Correlation Coefficient			Speed improvement percentage
	Strong	Medium	Weak	
Original 3DES	5.4%	36.3%	58.3%	47.25%
Enhanced 3DES Algorithm	6.4%	36.3%	57.3%	53.54%

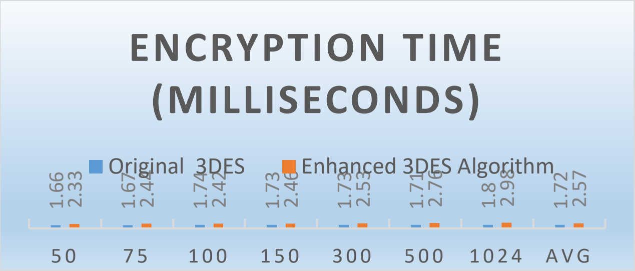


Figure 13. Encryption time for different text sizes (milliseconds)

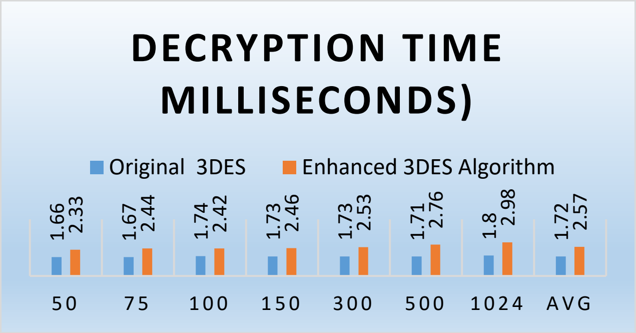


Figure 14. Decryption time for different text sizes (milliseconds).

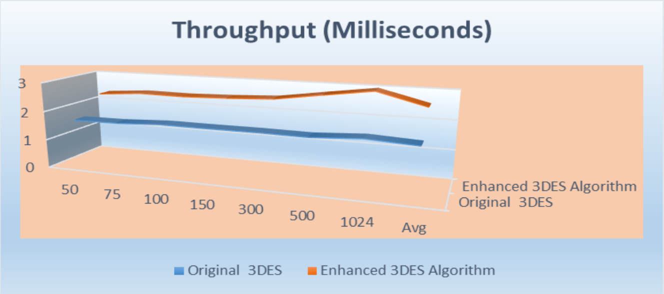


Figure 15. Throughput for different text sizes (Sec/MB).

VIII. ACKNOWLEDGMENT

The author expressed my gratitude to the Ministry of Education - Gifted Care Authority (www.https: //epedu.gov.iq/) Baghdad, Iraq, for their current support of this work.

IX. REFERENCES

[1]. Christy Atika Sari1, Eko Hari Rachmawanto2, Christanto Antonius Haryanto3, "Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security", Scientific Journal of Informatics , Vol. 5, No. 2, Nov 2018 p-ISSN 2407-7658 , e-ISSN 2460-0040Int. DOI: 10.15294/sji.v5i2.14844

[2]. Muhammad Faheem Mushtaq1 , Sapiee Jamel2 , Siti Radhiah B. Megat3 , Urooj Akram4 , Mustafa Mat Deris5 , "Key Schedule Algorithm using 3-Dimensional Hybrid Cubes for Block Cipher", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 8, 2019, (DOI) : 10.14569/IJACSA.2019.0100857

[3]. A. H. Disina, Z. A. Pindar, and S. Jamel, "Enhanced Caeser Cipher to Exclude Repetition and Withstand Frequency Cryptanalysis," J. Netw. Inf. Secur., 2015. Article can be accessed online at http://www.publishingindia.com

[4]. M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A Comprehensive Survey on the Cryptographic Encryption Algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 333–344, 2017, DOI: 10.14569/IJACSA.2017.081141.

[5]. M. F. Mushtaq, U. Akram, I. Khan, S. N. Khan, A. Shahzad, and A. Ullah, "Cloud Computing Environment and Security Challenges: A Review," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 10, pp. 183–195, 2017, (DOI) : 10.14569/IJACSA.2017.081025

[6]. A. H. Disina, S. Jamel, M. Aamir, Z. A. Pindar, M. M. Deris, and K. M. Mohamad, "A Key Scheduling Algorithm Based on Dynamic Quasigroup String Transformation and All-Or- Nothing Key Derivation Function," J. Telecommun. Electron. Comput. Eng., vol. 9, no. 3–5, pp. 1–6, Special Issue on Software Engineering III 2017, link https://jtec.utem.edu.my/jtec/article/view/2954

[7]. Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz Ali and Munam Ali Shah, " Cryptography: A Comparative Analysis for Modern Techniques," (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 8, No. 6, 2017, (DOI) : 10.14569/IJACSA.2017.080659.

[8]. S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advaces Inf. Sci., vol. 8, pp. 121–124, 2012, link https://www.researchgate.net/publication/275338264

[9]. Baha Eldin Hamouda Hassan Hamouda, " Comparative Study of Different Cryptographic Algorithms", Journal of Information Security, 2020, 11, 138-148 https://www.scirp.org/journal/jis ISSN Online: 2153-1242 ISSN Print: 2153-1234, DOI: 10.4236/jis.2020.113009.

[10]. M. Mikhail, Y. Abouelseoud, and G. Elkobrosy, "Extension and Application of El-Gamal Encryption Scheme," 2014. DOI: 10.1109/WCCAIS.2014.6916627

[11]. Nilesh, D., & Nagle, M, "The New Cryptography Algorithm with High Throughput", In Computer Communication and Informatics (ICCCI), 2014 International Conference on (pp. 1-5). IEEE, DOI: 10.1109/ICCCI.2014.6921739

[12]. Sangeeta and Er. Arpneek Kaur, "A Review on Symmetric Key Cryptography Algorithms", International Journal of Advanced Research in Computer Science, Volume 8, No. 4, May 2017 (Special Issue), DOI:https://doi.org/10.26483/ijarcs.v8i4.3777

[13]. Alaa A. Abdullatif, Firas A. Abdullatif , and Sinan A. Naji , " An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques," Periodicals of Engineering and Natural Sciences ISSN 2303-4521 Vol. 7, No. 4, December 2019, pp.1607-1617. DOI:http://dx.doi.org/10.21533/pen.v7i4.885.g429

[14]. M. Helmy, E.-S. M. El-Rabaie, I. M. Eldokany, and F. E. A. El-Samie, "3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm," 3D Research, vol. 8, no. 4, p. 38, 2017, DOI: 10.1007/s13319-017-0145-8

[15]. K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," Journal of Electrical and Computer Engineering, vol. 2012, p. 7, 2012, DOI: 10.1155/2012/173931 .

[16]. K. Abitha and P. K. Bharathan, "Secure Communication Based on Rubik's Cube Algorithm and Chaotic Baker Map," Procedia Technology, vol. 24, pp. 782-789, 2016, DOI: 10.1016/j.protcy.2016.05.089.

[17]. S. Kilaru, Y. Kanukuntla, A. Firdouse, and M. Bushra, "effective and key sensitive security algorithm for an image processing using robust Rubik encryption and decryption process," University of Birmingham, ISSN (Print), vol. 2, pp. 2278-8948, 2013, link http://www.irdindia.in/journal_ijaeee/pdf/vol2_iss5/17.pdf

[18]. Sheng Shou Puzzles. China Magic Cube. 2014. http://www.china-magic -cube.com/category/2.html.

[19]. Da Xing Zeng, M. Li, Juan, Yu Hou,and et," Overview of Rubik's Cube and Refections on Its Application in Mechanism", Chinese Journal of Mechanical Engineering, Zeng et al. Chin. J. Mech. Eng. (2018) 31:77 https://doi.org/10.1186/s10033-018-0269-7 springer .

Cite this article as :

Saadi Mohammed Saadi , "A Modern mechanism for Generating 3DES Algorithm Keys Based on Rubik's Cube", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 6, pp. 180-188, November-December 2022. Available at doi : https://doi.org/10.32628/IJSRSET22966
Journal URL : https://ijsrset.com/IJSRSET22966